UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,384	03/02/2000	Simon Robert Walmsley	AUTH07US	4249

7590 04/16/2004

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 04/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/517,384	Applicant(s) WALMSLEY, SIMON ROBERT
	Examiner Nga B. Nguyen	Art Unit 3628

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is the answer to the Amendment filed on February 4, 2004, which paper has been placed of record in the file.

2. Claims 1-16 are pending in this application.

Response to Arguments/Amendment

3. Applicant's arguments with respect to claims 1-16 have been considered but are not persuasive. In the arguments regarding to claim 1, applicant stated that Shin (US 5,987,134) does not disclose a comparison of an original and a decrypted random number from separate chips. Examiner respectfully disagrees. See Shin, column 9, line 35 through column 10, line 35, the verification device 10 (e.g. smart card reader-writer) generates a random number integer r having the value of C, the proving device 11 (e.g. smart card) generates the response R, the verification device then compares C and R to determine a match considering the proving device to be valid. Thus the original and a decrypted random number from separate chips (verification device and proving device) are compared. Moreover, applicant stated that the Shin's method is not the method claimed in the present application, but applicant did not show the differences between the steps claimed in the claim with the steps performing in the Shin's method. Shin meets all the steps claimed in the claim as addressed by examiner in the previous office action. Therefore, there is no distinguishes between the method claimed in the present invention with the Shin's method. Moreover, applicant did not file a terminal disclaimer

in compliance with 37 CFR 1.321(c), thus the provisional double patenting rejection is maintained.

In conclusion, for the reasons stated above, examiner decides to maintain the rejections described in the previous office action (also see details below) and make this action FINAL.

4. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claim 1 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 09/517,539. Although the conflicting claims are not identical, they are not patentably distinct from each other because claim 1 of copending Application No. 09/517,539 discloses the validation protocol for determining whether an untrusted authentication chip is valid using a one-way function (an asymmetric encryption function is a one-way function).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 3-5, 7-11, and 13-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Shin et al (hereinafter Shin), U.S. Patent No. 5,987,134.

Regarding to claim 1, Shin discloses a validation protocol for determining whether an untrusted authentication chip (column 9, lines 35-38, the proving device 11 is a smart card having an IC chip) is valid, or not, including the steps of:

generating a random number and encrypting with an asymmetric encryption function using a first key (column 9, lines 39-57 and column 28, lines 25-32, the verification device 10 generates a random number the RSA encryption function that is asymmetric encryption function);

passing the encrypted random number to an untrusted authentication chip (column 9, lines 50-57, the challenging data C is sent from the verification device 10 to the proving device 11) ;

decrypting the encrypted random number with an asymmetric decryption function using a secret key, in the untrusted authentication chip (column 9, line 58-column 10, lines 15);

comparing the decrypted random number with the original random number, and in the event of a match considering the untrusted chip to be valid (column 10, lines 15-33);

otherwise considering the untrusted chip to be invalid (column 10, lines 33-35).

Regarding to claim 3, Shin discloses the first key is a public key (column 8, lines 52-53).

Regarding to claim 4, Shin discloses the encryption is implemented in software (column 9, lines 9, lines 1-31).

Regarding to claim 5, Shin discloses the encryption is implemented in a second authentication chip (column 9, lines 31-34, a smart card reader-writer).

Regarding to claim 7, Shin discloses the system comprises:

a random number generator (figure 1, verification device 10 having random number generation means 102);

an asymmetric encryptor to encrypt generated random numbers and a first key for the encryptor (column 28, lines 1-3, 25-32);

an untrusted authentication chip includes an asymmetric decryption function to decrypt encrypted random number and a secret key for the decryption function (column column 9, line 58-column 10, line 15);

a comparison means are also provide to compare a decrypted random number with an original random number, and in the event of a match considering the untrusted chip to be valid; otherwise considering the untrusted chip to be valid; otherwise considering the untrusted chip to be invalid (column 10, lines 15-35 and column 36, lines 45-58).

Regarding to claims 8, 9, Shin discloses the random number generator, encryptor and comparison means are in an external system, the external system is in a device in which are mounted, and the untrusted chip is in the consumable (column 9,

lines 10-31, when the verification device is implemented as a program installed and executed on a server computer that is connected to a user's PC or workstation, thus the external system is the server computer and the untrusted chip is the user's PC)

Regarding to claim 10, Shin discloses the random number generator and encryptor are in a second authentication chip (column 9, lines 31-34, when the verification device is implemented as a program installed and executed on a smart card reader-writer), and the comparison means are in an external system which receives the random number and the encrypted version before passing only the encrypted version to the untrusted chip (column 36, lines 45-57); the system also receives back the decrypted version from the untrusted chip and performs the comparison (column 10, lines 12-25).

Regarding to claim 11, Shin discloses the system is in a device in which consumable are mounted, and the untrusted chip is in the consumable (column 9, lines 31-38, the system is a smart card reader-writer and the untrusted chip is a smart card).

Claims 13-15 contain similar limitations found in claims 3-5 discussed above, therefore are rejected by the same rationale.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2, 6, 12, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shin et al (hereinafter Shin), U.S. Patent No. 5,987,134.

Regarding to claims 2, 12, Shin discloses the random number is not secret, but where the trusted authentication chip contains a random function to produce random numbers from a seed (column 13, lines 10-11), but Shin does not disclose the function advances after every random number is produced so that the next random number will be produced from a new seed. However, it is well known to generate the next random number using a new seed in order to improve the level of security. Therefore, it would have been obvious to modify Shin's to include the feature above for the purpose of providing high security level because each next random number is generated from a new seed, thus the unauthorized person cannot easily to predict the random number.

Regarding to claims 6, 16, Shin does not disclose the keys used for encryption and decryption are 2048 bits or larger. However, it is well known to produce encryption or decryption keys using 2048 or larger bits. Therefore, it would have been obvious to modify Shin's to include the feature above for the purpose of providing high security level because producing the encryption and decryption keys with larger bits makes the unauthorized person cannot easily to guess the keys.

Conclusion

11. Claims 1-16 are rejected.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is

(703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

13. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

(703) 872-9326 (for formal communication intended for entry),

or

(703) 308-3691 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, Seventh Floor (Receptionist).

Nga B. Nguyen
April 15, 2004

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600